

Your Ref: 0023-0209JP

Our Ref: PA1120

**Translation of Selected Portions of
Pat. Laid-open Official Gazette**

Appln. No: 8-258440

Appln. Date: September 30, 1996

Laid-open Pub. No: 10-107795

Laid-open Pub. Date: April 24, 1998

Inventor(s): Mariko Kondo

Applicant(s): Hitachi Software Engineering K.K.

Attorney(s): Osayoshi Akita

1. Title of the Invention

NETWORK MANAGEMENT SYSTEM

2. Claims

(omitted)

3. Detailed Description of the Invention (Selected Portions)

1)

(omitted)

NETWORK MANAGEMENT SYSTEM

Publication number: JP10107795

Publication date: 1998-04-24

Inventor: KONDOU MARIKO

Applicant: HITACHI SOFTWARE ENG

Classification:

- international: G06F13/00; H04L12/24; H04L12/26; G06F13/00; H04L12/24; H04L12/26; (IPC1-7): H04L12/24; G06F13/00; H04L12/26

- European:

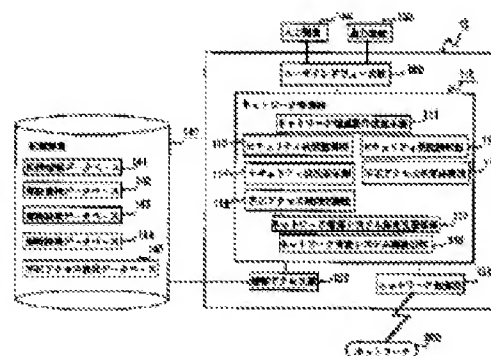
Application number: JP19960258440 19960930

Priority number(s): JP19960258440 19960930

[Report a data error here](#)

Abstract of JP10107795

PROBLEM TO BE SOLVED: To allow the system to detect an act by the network manager to destroy the security due to mistake or on purpose by monitoring the internal security according to a specific system. **SOLUTION:** A security status analysis section 113 analyzes monitor result data in a monitor result database 143 stored by a security status monitor section 112 and stores the result to an analysis result database 144. In the case of this analysis, such items as time, frequency of access, device security level and qualification of access party are checked and the result of analysis is stored based on a prescribed criterion. An illegal access discrimination processing section 115 discriminates the result of analysis of the analysis result database 144 as to whether the result comes from normal access or illegal access based on the criterion of an illegal access discrimination database 145. An illegal access tendency grasp section 116 analyzes the tendency of occurrence of illegal access and executes transaction such as alarming/access reject to the external network depending on the status.



Data supplied from the [esp@cenet](#) database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-107795

(43)公開日 平成10年(1998)4月24日

(51) Int.Cl.⁶

識別記号

FI

H04L 12/24

H0 4 L 11/08

12/26

G O 6 F 13/00

355

G O 6 F 13/00

3 5 5

審査請求 未請求 請求項の数7 OL (全 22 頁)

(21)出題番号

特願平8-258440

(22) 出題日

平成8年(1996)9月30日

(71)出願人 000233055

日立ソフトウェアエンジニアリング株式会
社

神奈川県横浜市中区尾上町6丁目81番地

(72)発明者 近藤 麻里子

神奈川県横浜市中区尾上町6丁目81番地
日立ソフトウェアエンジニアリング株式会
社内

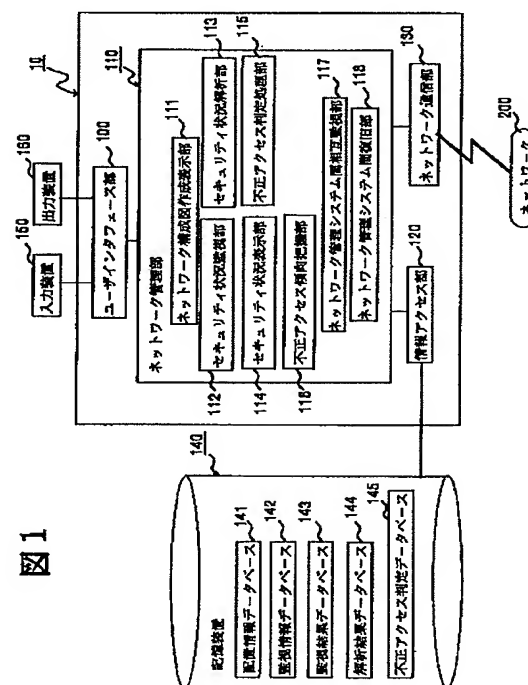
(74)代理人 弁理士 秋田 収喜

(54)【発明の名称】 ネットワーク管理システム

(57) 【要約】

【課題】 ネットワーク管理者の立場にある者が、故意または過失によりセキュリティを破壊する行為を検出すること。

【解決手段】 ネットワーク管理システムにおいて、配置情報データベースと、監視情報データベースと、監視結果データベースと、解析結果データベースとを備え、配置データベースに格納された情報に基づき、論理的または物理的なネットワーク構成図面を表示させるネットワーク構成図作成表示手段と、監視情報データベースに基づき、ネットワークにおける内部的なセキュリティ状況を監視し、その監視結果を監視結果データベースに格納する内部的セキュリティ状況監視手段と、監視結果データベースに格納された監視結果を基に、内部的なセキュリティ状況を解析し、その解析結果を解析結果データベースに格納する内部的なセキュリティ状況解析手段と、解析結果データベースを基に、ネットワークにおける内部的なセキュリティ状況を前記ネットワーク構成図面上に表示させる内部的セキュリティ状況表示手段を備える。



【特許請求の範囲】

【請求項1】 電子計算機を含む複数のネットワーク機器が接続されているネットワークを管理運用するネットワーク管理システムであって、

前記ネットワーク機器の物理的配置と接続関係に関する情報を格納する第1データベースと、前記電子計算機を含む複数のネットワーク機器の監視項目及び監視内容を格納する第2データベースと、前記第2データベースの内容に従った監視結果を格納する第3データベースと、前記第3データベースに格納された監視結果を、前記ネットワーク機器毎に、時刻、頻度、使用者情報に基づいて解析した解析結果を格納する第4データベースとを備え、

前記第1データベースに格納された情報に基づき、論理的または物理的なネットワーク構成図面を表示させるネットワーク構成図作成表示手段と、

前記第2データベースに基づき、前記ネットワークにおける内部的なセキュリティ状況を監視し、その監視結果を前記第3データベースに格納する内部的セキュリティ状況監視手段と、

前記第3データベースに格納された監視結果を基に、内部的なセキュリティ状況を解析し、その解析結果を前記第4データベースに格納する内部的なセキュリティ状況解析手段と、

前記第4データベースを基に、ネットワークにおける内部的なセキュリティ状況を前記ネットワーク構成図面上に表示させる内部的セキュリティ状況表示手段を備えたことを特徴とするネットワーク管理システム。

【請求項2】 前記請求項1に記載のネットワーク管理システムにおいて、前記第4データベースに格納された解析結果に関して、各々のアクセスが正常なものであるか、不正なものによるものかを判断するための判断基準を格納する第5データベースを備え、

前記第5データベースを基に、前記ネットワーク機器に対して不正アクセスが行われたか或いは行われているかを判定して、前記内部的セキュリティ状況表示手段により表示する不正アクセス判定手段を備えたことを特徴とするネットワーク管理システム。

【請求項3】 前記請求項2に記載のネットワーク管理システムにおいて、

前記不正アクセス判定手段で不正アクセスと判定された場合に、その不正アクセスに対する対策を行う手段を備えたことを特徴とするネットワーク管理システム。

【請求項4】 前記請求項1または請求項2のいずれかに記載されたネットワーク管理システムにおいて、前記セキュリティ状況表示手段は、そのセキュリティ状況、または不正アクセス判定における緊急度及び重要度に応じて表示形式を変えて表示する手段を備えたことを特徴とするネットワーク管理システム。

【請求項5】 前記請求項2に記載のネットワーク管理

システムにおいて、

前記第4データベースに格納する解析結果を一定期間蓄積し、その蓄積結果と前記第5データベースを用いて、前記ネットワーク機器に対する不正アクセスの傾向把握を行う不正アクセス傾向把握手段を備えたことを特徴とするネットワーク管理システム。

【請求項6】 前記請求項2に記載のネットワーク管理システムにおいて、

前記ネットワークが複数のサブネットワークで構成され、それらサブネットワークにそれぞれネットワーク管理システムが接続されている場合には、

各々のネットワーク管理システムが備えた前記第4データベースに格納された解析結果を相互にチェックし、あるネットワーク管理システムの管理下のサブネットワークで不正アクセスを検出した場合に、その不正アクセスが検出されたサブネットワークとのアクセスを一時中断するネットワーク管理システム間相互監視手段を備えたことを特徴とするネットワーク管理システム。

【請求項7】 前記請求項6に記載のネットワーク管理システムにおいて、

前記ネットワーク管理システム間相互監視手段により、一時的に中断しているサブネットワーク間のアクセスを不正アクセスに対する対策を行った後に復旧するネットワーク管理システム間復旧手段を備えたことを特徴とするネットワーク管理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワークを円滑に運用管理するためのネットワーク管理システムに関し、特に、ネットワークのセキュリティ管理を行うネットワーク管理システムに適用して有効な技術に関するものである。

【0002】

【従来の技術】ネットワークのセキュリティ管理に関する技術では、例えば、(1)特開平05-108487号公報の「コンピュータウィルス侵入防止装置と侵入防止方式」、(2)特開平06-337781号公報の「情報処理装置」、(3)特開平07-78179号公報の「情報ファイル装置」、(4)特開平07-99489号公報の「パスワード制御方法および装置」、(5)特開平07-248975号公報の「電子機器のセキュリティ保護装置」、(6)特開平07-262135号公報の「セキュリティ管理装置」、(7)特開平07-264178号公報の「セキュリティ方式」、などがある。

【0003】前記(1)のコンピュータウィルス侵入防止装置と侵入防止方式は、要求がコンピュータに取り込まれた時点で、正常かウィルスによるものかをウィルスの侵入事前チェックを行い判断するものである。

【0004】前記(2)の情報処理装置は、コンピュー

タウィルスのパターンを保存し、バッファに格納する入力データを比較し、一致した場合は、警報信号を送出し、インターフェイスを停止するものである。

【0005】前記(3)の情報ファイル装置は、画像情報検索の利用状況を履歴情報として記録し、一定件数(警告件数)以上の検索があった場合、警告表示し、最大件数まで達すると、媒体に保存するものである。

【0006】前記(4)のパスワード制御方法および装置は、使用装置に異常パスワードが次々入力された場合、データ保存し処理データを不定にし、2回又は5回固定パスワードを表示するものである。

【0007】前記(5)の電子機器のセキュリティ保護装置は、セキュリティ侵害検出機構で不正アクセスを検出し、電子機器内部のデータに対するアクセスの禁止やデータ消去により、データの盗用を防止するものである。

【0008】前記(6)のセキュリティ管理装置は、オープン型の分散ネットワーク環境でセキュリティオーディットサーバを設け、ネットワーク接続された機器からのセキュリティ侵害を検出した結果をレポート化し、その分析結果からセキュリティの弱点を診断し、セキュリティポリシーの改変要求を行うものである。

【0009】前記(7)のセキュリティ方式は、不正アクセスがネットワーク上の端末で行われた場合に、アラーム情報とアクセス履歴情報を用いて、どのLAN上に接続された端末かを特定するものである。

【0010】

【発明が解決しようとする課題】しかしながら、前記従来のネットワークのセキュリティ管理に関する技術は、ネットワークに不正侵入すること、または不正アクセスを行うことを防止することが主たる目的であったため、ネットワークを利用できる人(正規利用者)が悪用することを防止するといったことは考慮されておらず、以下に挙げるような問題点があった。

【0011】(1) ネットワーク管理システムの管理対象であるネットワーク接続された電子計算機やネットワーク機器の正規利用で、かつ、ネットワーク管理を行うネットワーク管理者の立場にある者が、ネットワーク管理を行う際に有する特権を用いて、故意または過失によりセキュリティを破壊する行為を行った場合に、それを検出できるものはない。

【0012】(2) 前記ネットワーク管理者が行う特権を用いたネットワーク管理作業において、正当な管理作業なのか、不正な行為なのかを判断できない。

【0013】(3) 前記ネットワーク管理者が行う特権を用いたネットワーク管理作業で不正アクセスが検出された場合に、ネットワーク上の他の電子計算機やネットワーク機器に対する安全性を確保する、即ち、セキュリティ対策を施せるものはない。

【0014】本発明の第一の目的は、ネットワーク管理システムの管理対象であるネットワーク接続された電子計算機やネットワーク機器の正規利用で、かつ、ネットワーク管理を行うネットワーク管理者の立場にある者が、ネットワーク管理を行う際に有する特権を用いて、故意または過失によりセキュリティを破壊する行為を行った場合に、それを検出することができるネットワーク管理システムを提供することである。

【0015】本発明の第二の目的は、ネットワーク管理者が行う特権を用いたネットワーク管理作業において、正当な管理作業なのか、不正な行為なのかを判断できるネットワーク管理システムを提供することである。

【0016】本発明の第三の目的は、ネットワーク管理者が行う特権を用いたネットワーク管理作業で不正アクセスが検出された場合に、ネットワーク上の他の電子計算機やネットワーク機器に対する安全性を確保する、即ち、セキュリティ対策を施せるネットワーク管理システムを提供することである。

【0017】

【課題を解決するための手段】本願において開示される発明のうち、代表的なものの概要を簡単に説明すれば、下記のとおりである。

【0018】電子計算機を含む複数のネットワーク機器が接続されているネットワークを管理運用するネットワーク管理システムであって、前記ネットワーク機器の物理的配置と接続関係に関する情報を格納する第1データベースと、前記電子計算機を含む複数のネットワーク機器の監視項目及び監視内容を格納する第2データベースと、前記第2データベースの内容に従った監視結果を格納する第3データベースと、前記第3データベースに格納された監視結果を、前記ネットワーク機器毎に、時刻、頻度、使用者情報に基づいて解析した解析結果を格納する第4データベースとを備え、前記第1データベースに格納された情報に基づき、論理的または物理的なネットワーク構成図面を表示させるネットワーク構成図作成表示手段と、前記第2データベースに基づき、前記ネットワークにおける内部的なセキュリティ状況を監視し、その監視結果を前記第3データベースに格納する内部的セキュリティ状況監視手段と、前記第3データベースに格納された監視結果を基に、内部的なセキュリティ状況を解析し、その解析結果を前記第4データベースに格納する内部的なセキュリティ状況解析手段と、前記第4データベースを基に、ネットワークにおける内部的なセキュリティ状況を前記ネットワーク構成図面上に表示させる内部的セキュリティ状況表示手段を備える。

【0019】また、前記第4データベースに格納された解析結果に関して、各々のアクセスが正常なものであるか、不正なものによるものかを判断するための判断基準を格納する第5データベースを備え、前記第5データベースを基に、前記ネットワーク機器に対して不正アクセ

スが行われたか或いは行われているかを判定して、前記内部的セキュリティ状況表示手段により表示する不正アクセス判定手段を備える。

【0020】さらに、前記ネットワークが複数のサブネットワークで構成され、それらサブネットワークにそれぞれネットワーク管理システムが接続されている場合には、各々のネットワーク管理システムが備えた前記第4データベースに格納された解析結果を相互にチェックし、あるネットワーク管理システムの管理下のサブネットワークで不正アクセスを検出した場合に、その不正アクセスが検出されたサブネットワークとのアクセスを一時中断するネットワーク管理システム間相互監視手段を備える。

【0021】

【発明の実施の形態】以下、本発明の実施例を図面を参照して具体的に説明する。

【0022】図1は本発明の一実施形態にかかるネットワーク管理システムの構成を説明するための機能ブロック図である。

【0023】図1に示すように、本実施形態のネットワーク管理システム10は、キーボード、マウスなどの入力装置150とディスプレイ、プリンタ、スピーカなどの出力装置160と接続され、データの入出力を制御するユーザインターフェイス部100と、ネットワーク（内部ネットワーク）200に接続された管理対象機器を管理するネットワーク管理部110と、ハードディスク、磁気テープ、光磁気ディスクなどの記憶装置140の情報をアクセスする情報アクセス部120と、ネットワーク200と接続され、その通信を制御するネットワーク通信部130とからなる。

【0024】上述したネットワーク管理部110は、図1に示すように、ネットワーク構成図を作成して表示するネットワーク構成図作成表示部111と、ネットワーク200の内部的なセキュリティ状況を監視するセキュリティ状況監視部112と、ネットワーク200の内部的なセキュリティ状況を解析するセキュリティ状況解析部113と、ネットワーク構成図作成表示部111で作成表示されたネットワーク構成図面上に内部的なセキュリティ状況を表示するセキュリティ状況表示部114と、ネットワーク200内部で不正アクセスが行われているか判定する不正アクセス判定部115と、不正アクセスに関する解析結果を蓄積し、その結果から傾向把握を行う不正アクセス傾向把握部116と、ネットワーク管理システム10が相互に不正アクセスを監視し、あるネットワーク管理システムの管理下のサブネットワークで不正アクセスを検出した場合に、その不正アクセスが検出されたサブネットワークとのアクセスを一時中断するネットワーク管理システム間相互監視部117と、不正アクセスを検出したネットワークとの通信を復旧するネットワーク管理システム間復旧部118とからなる。

【0025】また、記憶装置140は、図1に示すように、ネットワーク管理システム10が管理する管理対象機器（電子計算機、ネットワーク機器、端末、ケーブル）などの物理的配置と接続関係に関する情報を格納する配置情報データベース141（第1データベース）と、ネットワーク管理システム10の管理対象機器である電子計算機またはネットワーク機器に関するセキュリティ管理のための監視項目及び監視内容を格納する監視情報データベース142（第2データベース）と、監視情報データベース142に格納する監視項目と監視内容に従って、管理対象機器を監視した結果を格納する監視結果データベース143（第3データベース）と、監視結果データベース143に格納する監視結果をチェックし解析した結果を格納する解析結果データベース144（第4データベース）と、解析結果データベース144に格納された解析結果が正常なアクセスによるものか、不正なアクセスによるものかを判断するための判断基準を格納する不正アクセス判定データベース145（第5データベース）とからなる。

【0026】図2は、本実施形態のネットワーク管理システム10の管理対象である内部ネットワーク200の全体構成を説明するための模式的構成図である。図2において、300はネットワーク管理システム10の管理対象外である外部ネットワーク、301は外部ネットワーク300とネットワーク管理システム10の管理対象である内部ネットワーク200とを接続するファイアウォール、302はネットワーク管理システム10の管理対象である内部サブネットワークが複数接続する内部ネットワーク200の基幹ネットワーク部、303a～cはネットワーク管理システム10が管理する内部サブネットワークA、B、Cである。

【0027】本実施形態における内部ネットワーク200とは、ファイアウォール301の基幹ネットワーク部302との接続部分から、内部サブネットワークA303a、内部サブネットワークB303b、内部サブネットワークC303cまでを含めたものである。

【0028】ここで、ファイアウォール301は、外部ネットワーク300と内部ネットワーク200間の通信を制御し、内部から外部へ出ていく情報や、外部から内部に入ってくる情報の監視を行うものである。

【0029】また、基幹ネットワーク部302は、通常高速LANと呼ばれる数10～数100Mbps程度の転送速度を有するネットワークで、各内部サブネットワーク303間の通信や、内部サブネットワーク303から外部への通信に利用される。この基幹ネットワーク部の形状は、図3のようなバス型以外に、スター型、あるいは、リング型で構成される場合もある。

【0030】なお、内部ネットワーク200は、ファイアウォール301により外部ネットワーク300から守られており、外部ネットワーク300からの不正侵入や

情報盗聴は発生しないものとする。また、基幹ネットワーク部302に複数の内部サブネットワークA303a、B303b、C303cが接続した構成になっており、これら内部サブネットワークA303a、B303b、C303c間では相互通信が可能になっているものとする。

【0031】図3は、本実施形態のネットワーク管理システム10の管理対象となる上述した内部サブネットワーク303の論理的なネットワーク構成とネットワーク管理システム10の関係を説明するための模式的構成図である。

【0032】論理的ネットワーク構成とは、ネットワーク上で電子計算機、端末、ネットワーク機器、周辺機器がどのように接続しているかを示すものである。

【0033】図3において、401は基幹ネットワーク部400と内部サブネットワーク303を接続する基幹ネットワーク接続機器であり、402は内部サブネットワーク303の通信網であり、403は内部サブネットワーク303で使用するハブ等のネットワーク機器であり、404は端末であり、405は電子計算機である。

【0034】図3に示したように、本実施形態のネットワーク管理システム10は、基幹ネットワーク接続機器401を介して、基幹ネットワーク部302に接続する通信網402と、その通信網402に接続しているネットワーク機器403、端末404、電子計算機405を管理対象とする。

【0035】また、図3に示した内部サブネットワーク303とは、ネットワーク管理システム10の管理対象である通信網402と、ネットワーク機器403と、端末404と、電子計算機405と、基幹ネットワーク部302への接続を行う基幹ネットワーク接続機器401とまでを含めたものであり、各内部サブネットワーク303a~303cには、必ずその内部サブネットワーク303を管理する図1に示すネットワーク管理システム10が接続されている。

【0036】図3に示したネットワーク管理システム10は、接続されている内部サブネットワーク303の通信網402を流れている全ての通信内容を監視（モニタリング）し、その内容を解析する。

【0037】さらに、ネットワーク管理システム10は、通信網402を介して、各々の電子計算機405、ネットワーク機器403、端末404の通信内容や、稼働しているプログラムやコマンド群をモニタリングし、その内容を解析する。

【0038】これらの解析を実現するために、本実施形態のネットワーク管理システム10は、特権モードで稼働する。特権モードとは、他の如何なるプログラムやコマンドに対しても、特権的な動作が可能な状態のことである。特権モードで稼働する場合、一般のユーザに対し書き込みを禁止しているファイルの書換えや、他のユー

ザが起動しているプログラムの強制停止といった動作が行える。

【0039】また、本実施形態のネットワーク管理システム10の特権モードでの稼働は、ネットワークや電子計算機の管理を目的としたログイン名（ユーザID）を使用する特権ユーザにより可能となる。

【0040】また、図3に示す各内部サブネットワークA303a、B303b、C303cで稼働するネットワーク管理システム10は、相互に通信し、互いの保持する情報を交換する。

【0041】次に、図1に示した各データベース141~145の構成について説明する。

【0042】図4は、配置情報データベース141の構成を示す図である。配置情報データベース141には、ネットワーク管理システム10が管理する電子計算機405、ネットワーク機器403、端末404、通信網（ケーブル）402などの物理的配置と接続関係に関する情報を格納する。図4に示すように、配置情報データベース141には、ネットワーク管理システム10の管理対象機器である電子計算機405、ネットワーク機器403、端末404、ケーブル402一つ一つに対して付けられたユニークな番号である管理対象ID601と、後述するネットワーク構成図上の物理的位置を表す配置情報602と、電子計算機405、ネットワーク機器403、端末404、ケーブル402間の接続関係を表す接続情報603とが格納される。

【0043】図5は、監視情報データベース142の構成を示す図である。監視情報データベース142にはネットワーク管理システム10の管理対象機器である電子計算機405またはネットワーク機器403に関するセキュリティ管理のための監視項目及び監視内容を格納する。図5に示すように、監視情報データベース142には、図4の601と同様に、ネットワーク管理システム10の管理対象機器である電子計算機405やネットワーク機器403に対して付けられたユニークな番号である管理対象ID701と、その管理対象ID701で示される電子計算機405やネットワーク機器403に対して、どのような項目を監視するかを示す監視項目702と、その監視項目702に対してどのような監視を行うかを示す監視内容703とが格納される。

【0044】図6は、監視結果データベース143の構成を示す図である。監視結果データベース143には、図5に示した監視情報データベース142に格納する監視項目702と監視内容703に従って、管理対象機器を監視した結果を格納する。図6に示すように、監視結果データベース143には、図4の601及び図5の701と同様に、ネットワーク管理システム10の管理対象機器である電子計算機405やネットワーク機器403に対して付けられたユニークな番号である管理対象ID801と、図5の701と同様に、管理対象機器の監

視項目802と、ネットワーク管理システム10が図5の監視情報データベース142に格納された監視項目702と監視内容703に従って、管理対象ID801の電子計算機405やネットワーク機器403に対して監視した結果である監視結果803とが格納される。監視結果803は、監視項目802別に時系列にソートして格納される。

【0045】図7は、解析結果データベース144の構成を示す図である。解析結果データベース144は、図6の監視結果データベース143に格納する監視結果803を以下のようなチェック項目に基づき解析した結果を解析結果として格納する。

- 【0046】(1) いつ監視すべき事象が発生したか
- (2) どの位の頻度で監視すべき事象が発生しているか
- (3) どこで監視すべき事象が発生したか
- (4) 誰が監視すべき事象を発生させたか

図7に示すように、解析結果データベース144には、解析を行ったネットワーク管理システム10のID900と、監視対象である電子計算機405やネットワーク機器403の管理対象ID901と、図5の702と同様の管理対象機器に対する監視項目902と、その監視項目902に関する監視結果903と、その監視結果903に対して、上述したチェック項目の解析による解析結果904とが格納される。

【0047】図8は、不正アクセス判定データベース145の構成を示す図である。不正アクセス判定データベース145は、図7の解析結果データベース143に格納する解決結果904正常なアクセスによるものか不正なアクセスによるものかを判断するための判断基準を格納する。図8に示すように、不正アクセス判定データベース145には、図5の702と同様の管理対象に対する監視項目1001と、判断条件1002と、監視項目1001の解析結果904が判断条件1002に合致した場合の判定結果を表す判定1003と、監視項目1001に関する不正アクセスが行われたときの緊急度1004と、監視項目1001に関する不正アクセスが行われたときの重要度1005と、判定1003で不正と判定した場合の対策1006とが格納される。

【0048】次に、上述したネットワーク管理部110の各部112～118の処理について説明する。

【0049】まず、ネットワーク管理システム10が管理対象である電子計算機405やネットワーク機器403に対して行う内部的なセキュリティ状況の動的監視を行うセキュリティ状況監視部112のセキュリティ状況監視処理について図9に示したフローチャートを用いて説明する。

【0050】セキュリティ状況監視処理は、まず、入力装置150から内部的なセキュリティ状況の動的監視を行うネットワーク名をネットワーク管理システム10のユーザにより入力を受け(ステップ1100)、ネット

ワーク構成図作成表示部111により出力装置160に、ステップ1100で入力されたネットワーク名のネットワークのネットワーク構成図を表示する(ステップ1101)。

【0051】このネットワーク構成図とは、管理対象機器とそれらの接続をそれぞれの物理的な配置図と共に表示して示すものであり、その表示例として、図10に示すようなものが挙げられる。

【0052】この図10のネットワーク構成図では、図3に示した通信網402と、ネットワーク機器403と、端末404と、電子計算機405とがオフィス等のフロア図と共に表示してある。

【0053】次に、ステップ1101で表示したネットワーク内に含まれる管理対象機器に関する情報を、図4の配置情報データベース141から検索し(ステップ1102)、その検索した管理対象機器に関する情報を用いて、図5の監視情報データベース142から管理対象機器の監視内容を検索する(ステップ1103)。

【0054】その後、ステップ1103において検索した監視内容に従った管理対象機器での監視が行われているかをネットワーク通信部130にて確認し(ステップ1104)、その確認の結果を判断する(ステップ1105)。

【0055】管理対象機器において、内部的なセキュリティ状況を監視中でなかった場合は、ステップ1106へ進み、監視中であった場合は、ステップ1107へ進む。

【0056】ステップ1106では、ネットワーク管理システム10が管理対象機器において監視を開始させる。監視を開始させると、ネットワーク管理システムは、監視結果を図6の監視結果データベース143に監視項目別に時系列にソートして格納する。これは、ネットワーク管理システム10のユーザが監視中断の指示をするまでは監視が継続される。

【0057】ステップ1107では、ネットワーク管理システム10のユーザからの監視中断の指示があった場合、監視を終了する。

【0058】このように、ネットワーク管理システム10では、常時、図9に示すような内部的なセキュリティ状況の動的監視を行っている。

【0059】次に、ネットワーク200の内部的なセキュリティ状況を解析するセキュリティ状況解析部113のセキュリティ状況監視処理について図11に示したフローチャートを用いて説明する。

【0060】セキュリティ状況解析処理は、まず、内部的なセキュリティ状況の動的監視を行っている管理対象機器に関する監視結果が格納された図6の監視結果データベース143を検索し、管理対象機器が存在するかをチェックする(ステップ1200)。管理対象機器が存在する間は、ステップ1201へ進み、存在しなくなる

10

20

30

40

50

と処理を終了する。

【0061】ステップ1200で管理対象機器が存在する場合、図6の監視結果データベース143を検索し、管理対象機器の監視項目802別の監視結果803が存在するかをチェックする(ステップ1201)。監視項目802が存在する間は、ステップ1203へ進み、存在しなくなると、監視結果データベース143から次の管理対象機器を検索し、ステップ1200に戻る(ステップ1202)。

【0062】ステップ1201で管理対象機器の監視項目802が存在する場合、管理対象機器の監視項目802別の監視結果803が存在するかをチェックする(ステップ1203)。監視結果803が存在しなくなると、監視結果データベース143から次の監視項目802を検索し、ステップ1201に戻る(ステップ1205)。

【0063】ステップ1203で管理対象機器の監視結果803が存在する場合、以下のようなチェック項目に基づき監視結果803を解析し、監視すべき各事象に関する解析結果を、解析を行ったネットワーク管理システムの管理と共に、図7の解析結果データベース144に格納する(ステップ1204)。

- 【0064】(1) いつ監視すべき事象が発生したか
- (2) どの位の頻度で監視すべき事象が発生しているか
- (3) どこで監視すべき事象が発生したか
- (4) 誰が監視すべき事象を発生させたか

ここに示したチェック項目を具体的に説明すると、

(1) は、就業時間内か、時間外か、特に、深夜や早朝かどうかの解析を行う。(2) は、同一の操作を複数回行い何等かのエラーを発生させていないか、毎日決まった時刻に特定のプロセスが起動されていないか、等の解析を行う。(3) は、アクセス権を有する管理対象機器に対するアクセスか、一般のアクセス許諾設定のされている端末かどうか、等の解析を行う。(4) は管理者かどうか、特定のプロジェクトの構成員か、一般ユーザかどうかの解析を行う。

【0065】そして、ステップ1204において、監視結果803の解析が終了すると、ステップ1206に進み、監視結果データベース143から次の監視結果803を検索し、ステップ1203に戻る。

【0066】このように、ネットワーク管理システム10は、常時、図11に示した監視結果803の解析を行っている。

【0067】次に、ネットワーク構成図面上に緊急度及び重要度に応じてネットワーク200の内部的なセキュリティ状況を表示するセキュリティ状況表示部114のセキュリティ状況表示処理について図12と図13を用いて説明する。

【0068】セキュリティ状況表示部処理は、図12に示すように、まず、内部的なセキュリティ状況を表示す

るネットワーク名を入力装置150からユーザにより入力を受け(ステップ1300)、ステップ1300で入力されたネットワーク名のネットワークのネットワーク構成図(図10参照)を出力装置160に表示する(ステップ1301)。

【0069】次に、ステップ1301で表示したネットワーク内でセキュリティ状況の動的監視と監視結果の解析を行っている管理対象機器が格納された図7の解析結果データベース144を検索し、管理対象機器の解析結果904が存在するかをチェックする(ステップ1302)。解析結果904が存在する間は、ステップ1303へ進み、存在しなくなると処理を終了する。

【0070】ステップ1302で管理対象機器の解析結果904が存在する場合、不正アクセス判定条件を格納した図8の不正アクセス判定データベース145を検索し、図7の解析結果データベース144に格納した解析結果904との比較を行い、不正かどうかの判定を行う(ステップ1303)。

【0071】不正の場合はステップ1305へ進み、正常の場合はステップ1304において、解決結果データベース144から次の解析結果904を検索し、ステップ1302に戻る。

【0072】ステップ1303で管理対象機器の監視項目に関する解析結果904が不正であった場合、ステップ1305において、図8の不正アクセス判定データベース145に格納している緊急度1004と重要度1005に関して以下のレベルに従い、ステップ1301で表示したネットワーク構成図上に解析結果と不正アクセス判定結果を内部的なセキュリティ状況として表示する。

【0073】(1) 緊急度に関して：

- A) 即時：表示色変更・表示サイズ変更・点滅表示
- B) 緊急：表示色変更・表示サイズ変更
- C) 一般：表示色変更

(2) 重要度に関して：

- A) 最重要：表示色変更・表示サイズ変更・点滅表示
- B) 重要：表示色変更・表示サイズ変更
- C) 一般：表示色変更
- D) 注意：ウォーニング表示

この緊急度を具体的に説明すると、例えば、管理対象機器のシステム自体の変更を伴うものはA)の即時、ファイルの急激な膨張によるディスク・フルを生じさせるものはB)の重要、上述のA)とB)以外の不正アクセスはC)の一般となる。

【0074】また、重要度を具体的に説明すると、例えば、管理対象機器のシステム関連ファイルに関するものはA)の最重要、管理者のみがアクセス許諾されているものはB)重要、一般ユーザがアクセスできるものはC)の一般、誰にでもアクセスを許諾しているものはD)の注意となる。

【0075】次に、上述した解析結果の具体的な表示例について説明する。図13は、ネットワーク構成図面上の内部的なセキュリティ状況の表示例を示す図である。図13において、1400は通信網、1401はネットワーク機器、1402は電子計算機、1403は端末、1404は緊急レベルのセキュリティ状況にある被管理機器、1405は最重要レベルのセキュリティ状況にある被管理機器である。このように解析結果の表示を行う。

【0076】なお、ここで述べたネットワーク管理システムがネットワーク構成図面上に緊急度及び重要度に応じた表示による内部的なセキュリティ状況の表示処理は、図12で説明した解析処理の結果だけではなく、後述の図15に示す不正アクセスの傾向把握処理の結果、図17に示すネットワーク管理システムの相互監視処理の結果についても、同様に表示可能である。

【0077】次に、ネットワーク200において不正アクセスが行われたか或は行われているかを判定する不正アクセス判定処理部115の不正アクセス判定処理について図14のフローチャートを用いて説明する。

【0078】不正アクセス判定処理は、図14に示すように、まず、内部的なセキュリティ状況の動的監視を行っている管理対象機器に関する解析結果が格納された図7の解析結果データベース144を検索し、管理対象機器の解析結果904が存在するかをチェックする(ステップ1500)。解析結果904が存在する間は、ステップ1501へ進み、存在しなくなると処理を終了する。

【0079】ステップ1500で管理対象機器の解析結果が存在する場合、不正アクセス判定条件を格納した図10の不正アクセス判定データベース145を検索し、図7の解析結果データベース144に格納した監視項目902に関する解析結果904と比較を行い、不正かどうかの判定を行う(ステップ1501)。

【0080】不正の場合はステップ1503へ進み、正常の場合はステップ1502において、解析結果データベース144の解析結果904を検索し、ステップ1500に戻る。

【0081】ステップ1501で管理対象機器の監視項目902に関する解析結果が不正であった場合、図10の不正アクセス判定データベース145の不正アクセスに対する対策1006が存在するとき、その処理を行う(ステップ1503)。

【0082】ステップ1503で不正アクセスへの対策処理が終了するとステップ1502に進み、図7の解析結果データベース144から次の解析結果を検索し、ステップ1500に戻る。

【0083】次に、ネットワーク管理システム10が監視結果を一定期間蓄積し、その蓄積結果から不正アクセスの傾向把握を行う不正アクセス傾向把握部116にお

ける不正アクセス傾向把握処理について図15のフローチャートを用いて説明する。

【0084】不正アクセス傾向把握処理は、図15に示すように、まず、入力装置150から内部的なセキュリティ状況の動的監視を行うネットワーク名をネットワーク管理システム10のユーザにより入力を受け(ステップ1600)、ネットワーク構成図作成表示部111により出力装置160に、ステップ1100で入力されたネットワーク名のネットワークのネットワーク構成図を表示する(ステップ1601)。

【0085】次に、ステップ1601で表示したネットワーク内でセキュリティ状況の動的監視と監視結果の解析を行っている管理対象機器に関する解析結果を格納した図7の解析結果データベース144を検索し、管理対象機器の解析結果904が存在するかをチェックする(ステップ1602)。解析結果904が存在する間は、ステップ1603へ進み、存在しなくなると処理を終了する。

【0086】ステップ1602で管理対象機器の解析結果904が存在する場合、不正アクセス条件が格納された図10の不正アクセス判定データベース145を検索し、図7の解析結果データベース144の監視項目902に関する解析結果904と比較を行い、不正かどうかの判定を行う(ステップ1603)。

【0087】不正の場合はステップ1605へ進み、正常の場合はステップ1604において、解析結果データベース144から次の解析結果904を検索し、ステップ1602に戻る。

【0088】ステップ1603で管理対象機器の監視項目902に関する解析結果904が不正だった場合、不正アクセスの傾向把握を行う(ステップ1605)。

【0089】この不正アクセスの傾向把握は、不正アクセスが行われる状況を掴むためのものであり一定期間中に発生した各事象を時系列に解析し、時間的、場所的な分布を算出する。これにより、不正アクセスの時間的、場所的な傾向を把握できる。

【0090】ステップ1605で不正アクセスの傾向把握が終了すると、ステップ1604に進み、図7の解析結果データベースの次の解析結果904を検索し、ステップ1602に戻る。

【0091】次に、複数のネットワーク管理システム10が稼働している場合に、各々のネットワーク管理システム10が相互に監視結果をチェックするネットワーク管理システム間相互監視部117におけるネットワーク管理システム間相互監視処理について説明する。

【0092】内部サブネットワーク303で稼働する複数のネットワーク管理システム10は各々、図3に示したような内部サブネットワーク303の管理に加えて、基幹ネットワーク302に接続されている他の内部サブネットワーク303において、セキュリティが確保され

ているかを、ネットワーク管理システム間相互監視部117において特権モードを用いて監視する。

【0093】そのネットワーク管理システム間相互監視処理は、他の内部サブネットワーク303で稼働しているネットワーク管理システム10が行っているセキュリティ状況の動的監視結果を用いて、他の内部サブネットワーク303でセキュリティが確保されているかどうかを相互に監視し合う処理である。

【0094】もし、不正なアクセスが他の内部サブネットワーク303で検出された場合は、その内部サブネットワーク303自体を信頼できないものと判断し、その内部サブネットワーク303に接続されているネットワーク機器403、端末404、電子計算機405からのアクセス要求を一時的に拒絶する。

【0095】これにより、不正アクセスの検出された内部サブネットワーク303は、他の内部サブネットワークとの通信が行えなくなり、内部ネットワーク303から孤立することになる。本来、ネットワーク接続は、情報や資源の共有、情報交換の高速化等を目的として行われるものであるため、内部ネットワーク200での孤立は、内部サブネットワーク303内のユーザにとって、内部ネットワーク200内で情報や資源の共有が行えず、高速な情報交換が行えなくなるという不利益が生じることになる。

【0096】さらに、ネットワーク管理システム10は不正アクセスを検出した他の内部サブネットワーク303内のユーザ全員に対し、その内部サブネットワーク303内で不正アクセスが行われている、即ち、セキュリティが確保されていないことを通知する。また、ある内部サブネットワーク303内のユーザが、不正アクセスを検出した他の内部サブネットワーク303に対してアクセス要求を行った場合も、そのユーザに対して、アクセス要求を行った他の内部サブネットワーク303は、セキュリティが確保されていないことを警告し、そのアクセス要求により、内部サブネットワーク303が危険に晒される可能性があることを通知する。

【0097】したがって、この仕組みを内部ネットワーク200全体で運用すると、ある内部サブネットワークにおいて、その内部サブネットワーク303内の特権を有する管理者が、その特権を用いて何らかの不正アクセスを行った場合に、その事実が内部ネットワーク200全体、更に、その内部ネットワーク200内の全ユーザに対して、公になる。

【0098】これにより、こうした不利益を内部サブネットワーク303内のユーザに対して被らせるような行為を、その内部サブネットワーク303の管理者が行ったことが公表されることが予め自明となるため、特権を有する管理者に対して、そうした不正行為を抑制させることが可能である。

【0099】ネットワーク管理者とはネットワーク接続

による利益を得るために、環境設定等を行う立場にいる人間であるため、自らの不正行為により不利益が生じると判っている事項を、あえて行うことはなくなる。

【0100】また、ネットワーク管理者が属する内部サブネットワーク303の全ユーザに、不正行為を通知されるため、ネットワーク管理者としての特権が剥奪される可能性が高くなる。つまり、自らの有している特権を失うことに繋がる行為を、故意にすることは考え難くなる。ネットワーク管理者における不正行為を防止できる。

【0101】さらに、ネットワーク管理システム10がそうした不正行為をその内部サブネットワーク303のユーザや、他の内部サブネットワーク303に対して公表することは、複数の内部サブネットワーク303の管理者間で、相互に信頼すべき管理者かどうかを監視することになるため、管理者間で協調して不正を行うことも困難である。

【0102】また、相互監視による内部サブネットワーク303の管理ではなく、各内部サブネットワーク303を統括するような、内部ネットワーク200の管理者、或は、内部ネットワーク200にネットワーク管理システムを置いて内部ネットワーク200全体を管理する場合は、その全体の管理者、即ち、最も強い権限を有する管理者の不正行為を検出することが非常に難しい。したがって、上位概念のネットワーク管理システムを用いて内部ネットワーク200を管理するのと比較して、相互監視による内部サブネットワーク303の管理は、安全性が高いと言える。

【0103】次に、上述したネットワーク管理システム間相互監視処理と監視結果をチェックする処理について、図16のフローチャートを用いて説明する。

【0104】ネットワーク管理システム間相互監視処理は、図16に示すように、まず、内部的なセキュリティ状況の動的監視を行っているネットワーク管理システム10を通信可能な他の内部サブネットワーク303のネットワーク管理システム10のネットワーク通信部130から検索する(ステップ1700)。

【0105】通信可能な他の内部サブネットワーク303上で稼働しているネットワーク管理システム10があれば、ステップ1701へ進み、存在しなければ処理を終了する。

【0106】ステップ1700で通信可能な他の内部サブネットワーク303上にネットワーク管理システム10がある場合、そのネットワーク管理システム10の解析結果が格納された図7の解析結果データベース144を検索し、管理対象機器の監視項目902別の解析結果904が存在するかをチェックする(ステップ1701)。監視項目902が存在する間は、ステップ1703へ進み、存在なくなるとステップ1702において、通信可能な次のネットワーク管理システム10を検

索し、ステップ1700に戻る。

【0107】ステップ1701で他の内部サブネットワーク303上で稼働するネットワーク管理システム10の管理対象機器の解析結果904が存在する場合、解析結果904を用いて図8の不正アクセス判定データベース145を検索し、現在検索しているネットワーク管理システム10が稼働している内部サブネットワーク303以外の他の内部サブネットワーク303に通知すべき事象、すなわち不正アクセスが管理対象機器で発生していないかどうかをチェックする(ステップ1703)。

もし、不正がある場合にはステップ1704へ進み、存在なくなるとステップ1705において、図7の解析結果データベース144から次の解析結果904を検索し、ステップ1701に戻る。

【0108】ステップ1703で管理対象機器の監視項目902に関する解析結果904が不正だった場合、内部サブネットワーク303上で稼働する全てのネットワーク管理システム10に対して、その内部サブネットワーク303内で何らかの不正アクセスを検出した旨、通知を行う。通知を受けた他のネットワーク管理システム10は、再度、通知元のネットワーク管理システム10から安全確認後の通知があるまで、通知元のネットワークとの通信を行わない(ステップ1704)。

【0109】不正アクセスを検出した内部サブネットワーク303との通信の一時的な中断は、通信内容に含まれる発信元アドレスをチェックすることで行う。つまり、発信元アドレスが不正アクセスが検出された内部サブネットワーク303のアドレスだった場合は、その通信内容を受け取らない、無視することになる。

【0110】ステップ1704において、複数のネットワーク管理システム10間での相互監視が終了すると、ステップ1706に進み、図7の解析結果データベース144から次の解析結果904を検索し、ステップ1703に戻る。

【0111】次に、上述の図16で説明したネットワーク管理システム10が内部サブネットワーク303を相互に監視する処理と監視結果をチェックする処理において、ある内部サブネットワーク303で不正アクセスを検出した場合に、通信不能だった内部サブネットワーク303が通信可能になる、即ち、不正アクセスに対する対策を実施した後、ネットワークに復旧するネットワーク管理システム間復旧部118のネットワーク管理システム間復旧処理について、図17のフローチャートを用いて説明する。

【0112】ネットワーク管理システム間復旧処理は、図17に示すように、まず、一定期間待つ(ステップ1800)。

【0113】次に、再度不正アクセスがあった内部サブネットワーク303で稼働しているネットワーク管理システム10の監視結果902及び解析結果903を再チ

ェックする(ステップ1801)。

【0114】ステップ1801で再チェックした内容に不正と判断すべき事象が含まれていない場合は1803へ進み、含まれている場合は通信を中断したままで、ステップ1800に戻る(ステップ1802)。したがって、ステップ1801の再チェックで不正が含まれなくなるまでは、不正アクセスがあった内部サブネットワーク303は、他の内部サブネットワーク303とは通信できない状態が続く。

【0115】その後、不正アクセスがあった内部サブネットワーク303の再チェック結果を、他の内部サブネットワーク303で稼働しているネットワーク管理システム10に通知する(ステップ1803)。

【0116】通知を受けとった他の内部サブネットワーク303のネットワーク管理システム10は、各々自身の判断基準で不正アクセスがあった内部サブネットワーク303で稼働しているネットワーク管理システム10の監視結果及び解析結果を再チェックし、通知を行ったネットワーク管理システム10と同様の結果が得られた場合は、通知を行ったネットワーク管理システム10に対し、再開承認通知を送付する。

【0117】その後、ネットワーク管理システム10は他の全ての内部サブネットワーク303で稼働しているネットワーク管理システム10から再開承認通知が届いたかをチェックし、全てのネットワーク管理システム10が承認した場合はステップ1806へ、まだ承認通知を送付していないネットワーク管理システム10がある場合は、ステップ1805へ進む。

【0118】ステップ1805で一定期間待ち、全てのネットワーク管理システム10から再開承認通知が届くまで、ステップ1804のチェックを繰り返す。

【0119】そして、全てのネットワーク管理システム10から再開承認通知が届いた時点で、通知を行ったネットワーク管理システム10は、通信を再開することを不正アクセスがあった内部サブネットワーク303を含めた、他の全てのネットワーク管理システム10に通知する。

【0120】最後に、上述の図16で説明したネットワーク管理システム間相互監視処理において、複数のネットワーク管理システム10の相互監視結果が食い違った場合の処理について説明する。

【0121】複数のネットワーク管理システム10が複数の内部サブネットワーク303上で稼働しているということは、常時どこかのネットワーク管理システム10が、他の内部サブネットワーク303を監視していることを意味する。したがって、ある内部サブネットワーク303上のネットワーク管理システム10が他の内部サブネットワーク303での不正アクセスを検出した場合に、別の内部サブネットワーク303上のネットワーク管理システム10は、異なる監視結果、即ち、不正アク

10

20

30

40

50

セスを検出しないことも考えられる。また、他の内部サブネットワーク303のネットワーク管理システム10の監視結果自体に不正があり、正常な解析や判断を行えない場合も想定される。

【0122】こうした場合に、本実施形態のネットワーク管理システム10は、以下の方法で不正を検出した内部サブネットワーク10に対する処理を行う。

【0123】まず、複数のネットワーク管理システム10は、図5の監視情報データベース142に監視項目702及び監視内容703を、図6の監視結果データベース143に監視結果803を、図7の解析結果データベース144に解析結果904を、図8の不正アクセス判定データベース145に不正アクセスの判断基準1002を、各々内部で保有している。なお、不正アクセス判定データベース145に格納する不正アクセスの判断基準1002は、内部ネットワーク200内で共通である。

【0124】したがって、あるネットワーク管理システム10が、他の内部サブネットワーク303の監視を行った時点での解析結果904が、別のネットワーク管理システム10の解析結果904と異なる場合は、最新の解析結果904を有するネットワーク管理システム10を信頼する。

【0125】但し、ある内部サブネットワーク303の管理者が特権を用いて、ネットワーク管理システム10自体に改竄を行い、不正の検出を正常に行っていない場合は、最新の解析結果904であっても信頼することはできない。

【0126】そこで、異なる解析結果904を有する、他の内部サブネットワーク303のネットワーク管理システム10があった場合、ネットワーク管理システム10は、異なる解析結果904のネットワーク管理システム10の有する図5の監視情報データベース142と、図7の解析結果データベース144の内容を、その他の内部サブネットワーク303で稼働するネットワーク管理システム10の有する各々の監視情報データベース143及び解析結果データベース144と比較する。

【0127】不正の検出結果及び解析結果904は、この監視情報データベース142及び解析結果データベース144に格納する情報によって異なるため、個々のネットワーク管理システム10間で差異がなければ、信頼できるものと判断する。

【0128】また、全てのネットワーク管理システム10が各々全く異なる解析結果904を有する場合は、どの内部サブネットワーク303も信頼できないことになり、結果的に、内部サブネットワーク303間の通信は、全く行われないことになる。

【0129】このような状況は、上述したようにネットワーク管理者はネットワーク接続のメリットを失う状況になることから考え難い。

【0130】したがって、多くのネットワーク管理システム10は、同一の解析結果904を導き出すと考えられ、結果として、最も同じ解析結果904となるネットワーク管理システム10が互いに信頼できることになる。

【0131】以上、説明したように、電子計算機を含む複数のネットワーク機器が接続されているネットワークを管理運用するネットワーク管理システムであって、前記ネットワーク機器の物理的配置と接続関係に関する情報を格納する配置情報データベースと、前記電子計算機を含む複数のネットワーク機器の監視項目及び監視内容を格納する監視情報データベースと、前記監視情報データベースの内容に従った監視結果を格納する監視結果データベースと、前記監視結果データベースに格納された監視結果を、前記ネットワーク機器毎に、時刻、頻度、使用者情報に基づいて解析した解析結果を格納する監視結果データベースとを備え、前記配置情報データベースに格納された情報に基づき、論理的または物理的なネットワーク構成図面を表示させるネットワーク構成図作成表示手段と、前記監視情報データベースに基づき、前記ネットワークにおける内部的なセキュリティ状況を監視し、その監視結果を前記監視結果データベースに格納する内部的セキュリティ状況監視手段と、前記監視結果データベースに格納された監視結果を基に、内部的なセキュリティ状況を解析し、その解析結果を前記解析結果データベースに格納する内部的なセキュリティ状況解析手段と、前記解析結果データベースを基に、ネットワークにおける内部的なセキュリティ状況を前記ネットワーク構成図面上に表示させる内部的セキュリティ状況表示手段を備えることにより、ネットワーク管理システムの管理対象であるネットワーク接続された電子計算機やネットワーク機器の正規の利用者で、かつ、ネットワーク管理を行うネットワーク管理者の立場にある者が、ネットワーク管理を行う際に有する特権を用いて、故意または過失によりセキュリティを破壊する行為を行った場合に、それを検出することができる。

【0132】また、前記解析結果データベースに格納された解析結果に関して、各々のアクセスが正常なものであるか、不正なものによるものかを判断するための判断基準を格納する不正アクセス判定データベースを備え、前記不正アクセス判定データベースを基に、前記ネットワーク機器に対して不正アクセスが行われたか或いは行われているかを判定して、前記内部的セキュリティ状況表示手段により表示する不正アクセス判定手段を備えることにより、ネットワーク管理者が行う特権を用いたネットワーク管理作業において、正当な管理作業なのか、不正な行為なのかを判断できる。

【0133】さらに、前記ネットワークが複数のサブネットワークで構成され、それらサブネットワークにそれぞれネットワーク管理システムが接続されている場合に

は、各々のネットワーク管理システムが備えた前記解析結果データベースに格納された解析結果を相互にチェックし、あるネットワーク管理システムの管理下のサブネットワークで不正アクセスを検出した場合に、その不正アクセスが検出されたサブネットワークとのアクセスを一時中断するネットワーク管理システム間相互監視手段を備えることにより、ネットワーク管理者が行う特権を用いたネットワーク管理作業で不正アクセスが検出された場合に、ネットワーク上の他の電子計算機やネットワーク機器に対する安全性を確保する、即ち、セキュリティ対策を施すことができる。

【0134】なお、上述したネットワーク管理システム10のネットワーク管理部110は、コンピュータで実行可能なプログラムで実現される場合もあり、そのときのプログラムは、フロッピーディスク、CD-ROM、マスクROM等の記憶媒体で一般ユーザに提供される。この場合、さらに、これら処理の他にGUIプログラム等の他のプログラムと組み合わせてユーザに提供することもある。

【0135】また、上述した記憶媒体で提供する代替手段として、インターネット等のネットワークを通じて有償で提供することもある。

【0136】以上、本発明者によってなされた発明を、前記実施形態に基づき具体的に説明したが、本発明は、前記実施形態に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能であることは勿論である。

【0137】

【発明の効果】本願において開示される発明のうち代表的なものによって得られる効果を簡単に説明すれば、下記のとおりである。

【0138】ネットワーク管理システムの管理対象であるネットワーク接続された電子計算機やネットワーク機器の正規の利用者で、かつ、ネットワーク管理を行うネットワーク管理者の立場にある者が、ネットワーク管理を行う際に有する特権を用いて、故意または過失によりセキュリティを破壊する行為を行った場合に、それを検出することができる。

【0139】また、ネットワーク管理者が行う特権を用いたネットワーク管理作業において、正当な管理作業なのか、不正な行為なのかを判断できる。

【0140】さらに、ネットワーク管理者が行う特権を用いたネットワーク管理作業で不正アクセスが検出された場合に、ネットワーク上の他の電子計算機やネットワーク機器に対する安全性を確保する、即ち、セキュリティ対策を施すことができる。

【図面の簡単な説明】

【図1】本発明の実施形態にかかるネットワーク管理シ

ステムのシステム構成を示す図である。

【図2】本実施形態のネットワークの全体構成を説明するための模式的構成図である。

【図3】本実施形態のネットワーク管理システムの管理対象となる内部サブネットの論理的なネットワーク構成を説明するための図である。

【図4】配置情報データベースの構成を示す図である。

【図5】監視情報データベースの構成を示す図である。

【図6】監視結果データベースの構成を示す図である。

【図7】解析結果データベースの構成を示す図である。

【図8】不正アクセス判定データベースの構成を示す図である。

【図9】セキュリティ状況監視処理を説明するフローチャートである。

【図10】ネットワーク構成図面の表示例を示す図である。

【図11】セキュリティ状況解析処理を説明するフローチャートである。

【図12】セキュリティ状況表示処理を説明するフローチャートである。

【図13】セキュリティ状況の表示例を示した図である。

【図14】不正アクセス判定処理を説明するフローチャートである。

【図15】不正アクセス傾向把握処理を説明するフローチャートである。

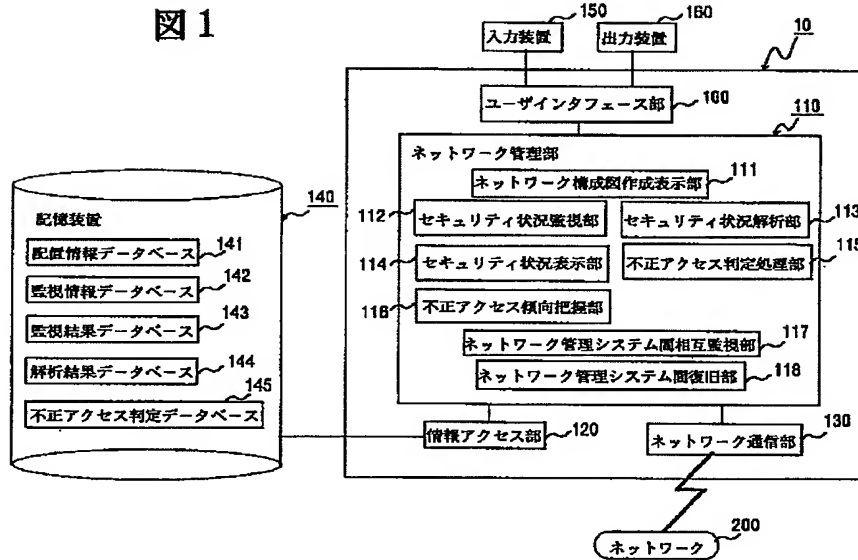
【図16】ネットワーク管理システム間相互監視処理を説明するフローチャートである。

【図17】ネットワーク管理システム間復旧処理を説明するフローチャートである。

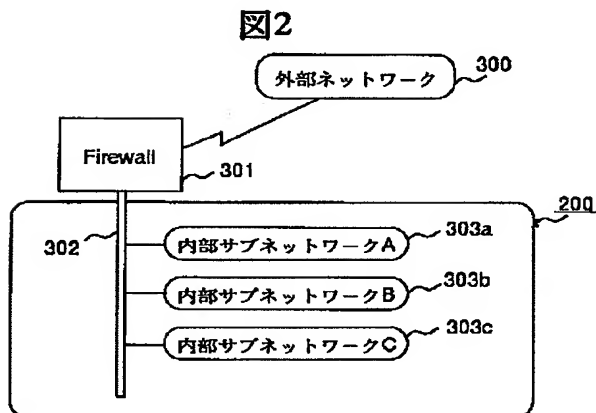
【符号の説明】

10…ネットワーク管理システム、100…ユーザインターフェイス部、110…ネットワーク管理部、111…ネットワーク構成図作成表示部、112…セキュリティ状況監視部、113…セキュリティ状況解析部、114…セキュリティ状況表示部、115…不正アクセス判定部、116…不正アクセス傾向把握部、117…ネットワーク管理システム間相互監視部、118…ネットワーク管理システム間復旧部、120…情報アクセス部、130…ネットワーク通信部、140…記憶装置、141…配置情報データベース（第1データベース）、142…監視情報データベース（第2データベース）、143…監視結果データベース（第3データベース）、144…解析結果データベース（第4データベース）、145…不正アクセス判定データベース（第5データベース）、150…入力装置、160…出力装置、200…ネットワーク。

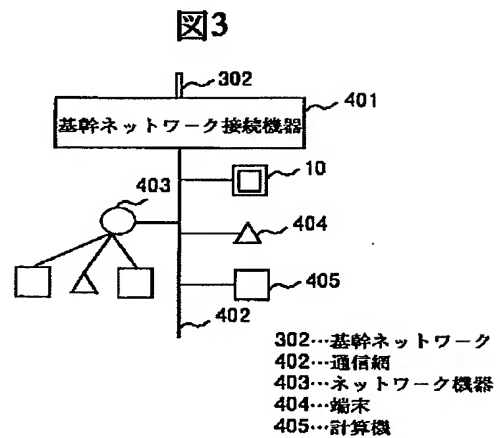
【図1】



【図2】



【図3】



【図5】

図5は、監視項目と監視内容の表である。

管理対象ID	監視項目	監視内容
11021	ログイン	常時ログ取得
26359	特権プロセス	SUIDチェック/週
:	:	:

142

【図4】

図 4

601 管理対象ID	602 配置情報	603 接続先ID
11021	東京本社ビル / 3F/x=20:y=45	24820
26359	東京本社ビル / 8F/x=58:y=12	620
:	:	:

141 ↗

【図6】

図 6

801 管理対象ID	802 監視項目	803 監視結果
511021	ログイン	1995/11/24 03:21:54 JST login from A to B (user C)
		1995/11/24 05:04:11 JST login from D to A (user E)
	:	:
126359	特権プロセス	1995/11/24 00:15:37 JST su from I to F (user H)
		1995/11/24 04:40:53 JST SUID proc X running at Y
	:	:
:	:	:

143 ↗

【図7】

図 7

管理ID	対象ID	監視項目	監視結果	解析結果
523452	656252	ログイン	1995/11/24 03:19:09 SU edit file A	就業時間外アクセス
523452	12353	特権プロセス	1995/11/24 03:21:54 SUID proc M	一般ユーザの特権プロセス起動
:	:	:	:	:

144

【図8】

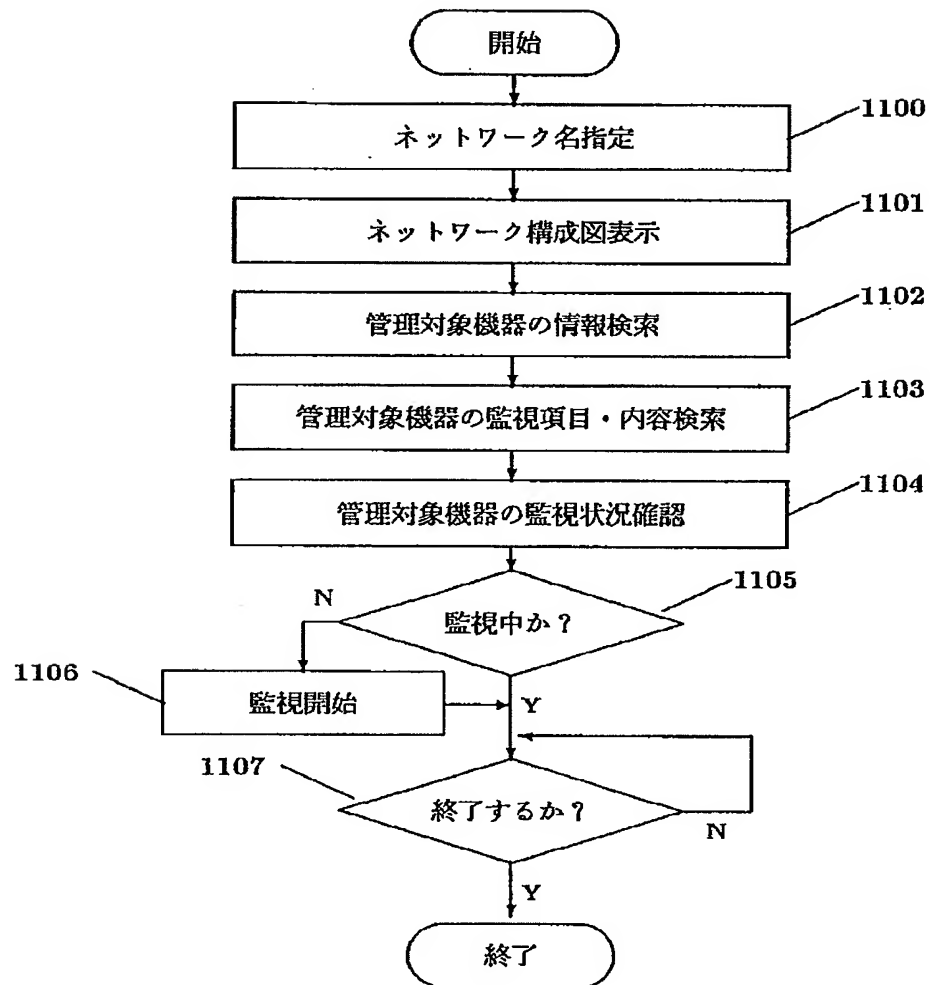
図 8

監視項目	判断条件	判定	緊急度	重要度	対策
ログイン	就業時間外アクセス	不正	一般	重要	追跡調査
	就業時間内アクセス	正常	—	—	—
特権プロセス	システム管理用ファイル更新	不正	緊急	最重要	強制終了
:	:	:	:	:	:

145

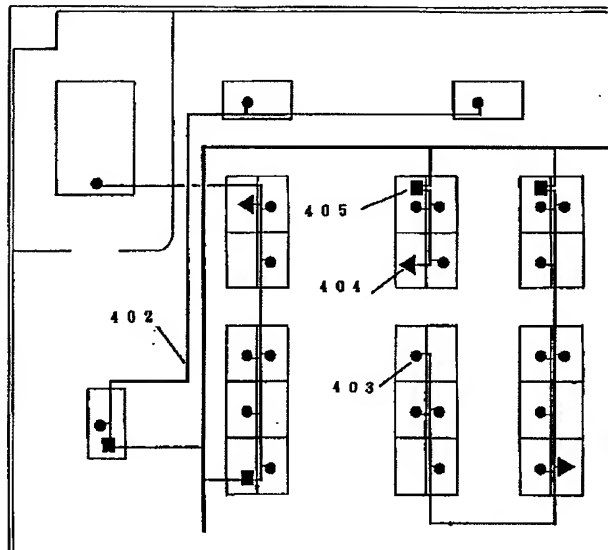
【図9】

図 9



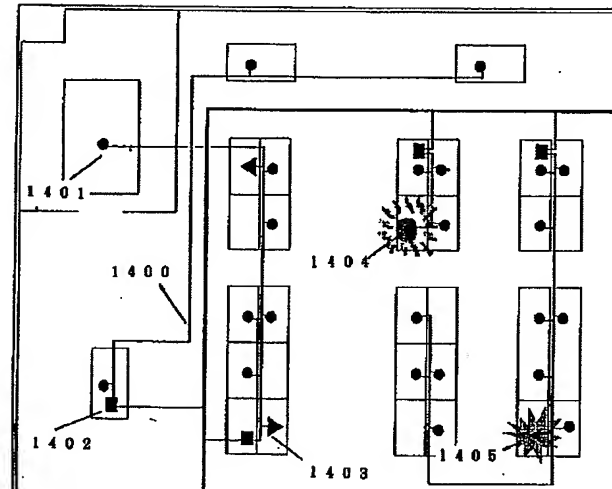
【図10】

図10



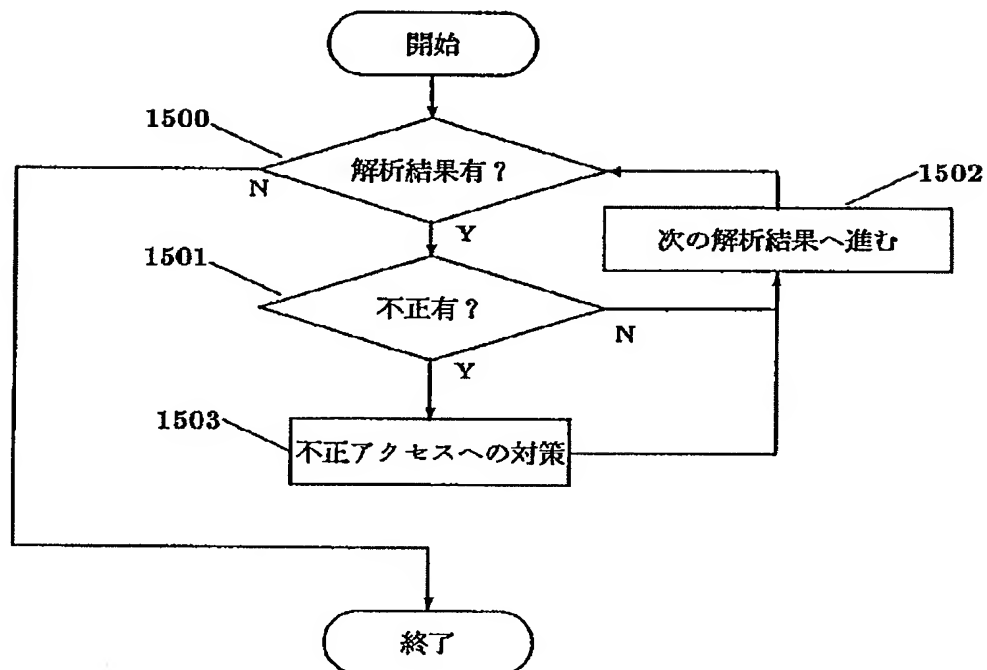
【図13】

図13



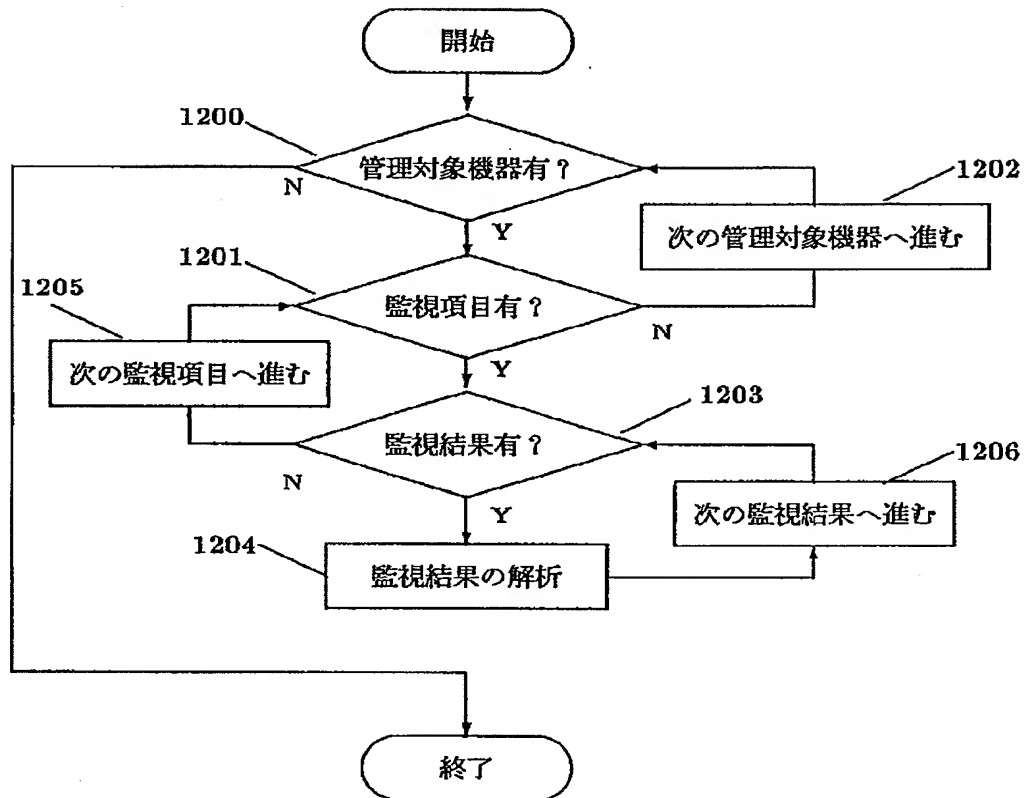
【図14】

図14



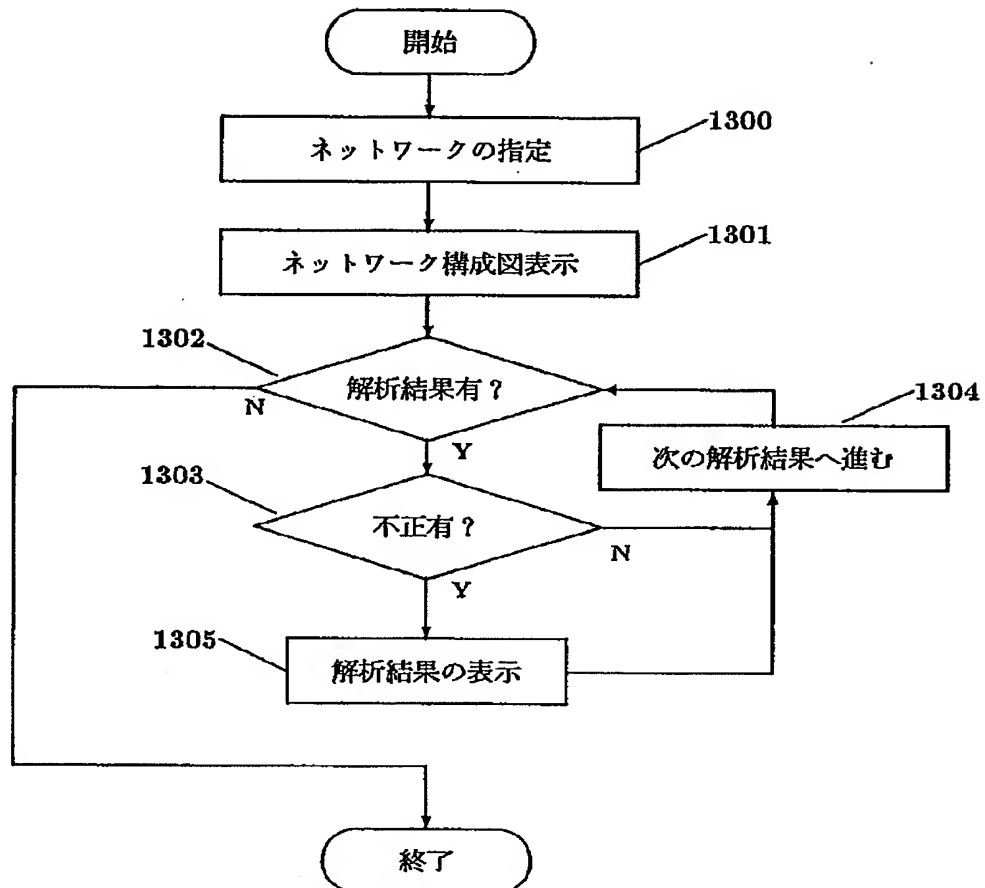
【図11】

図 1 1



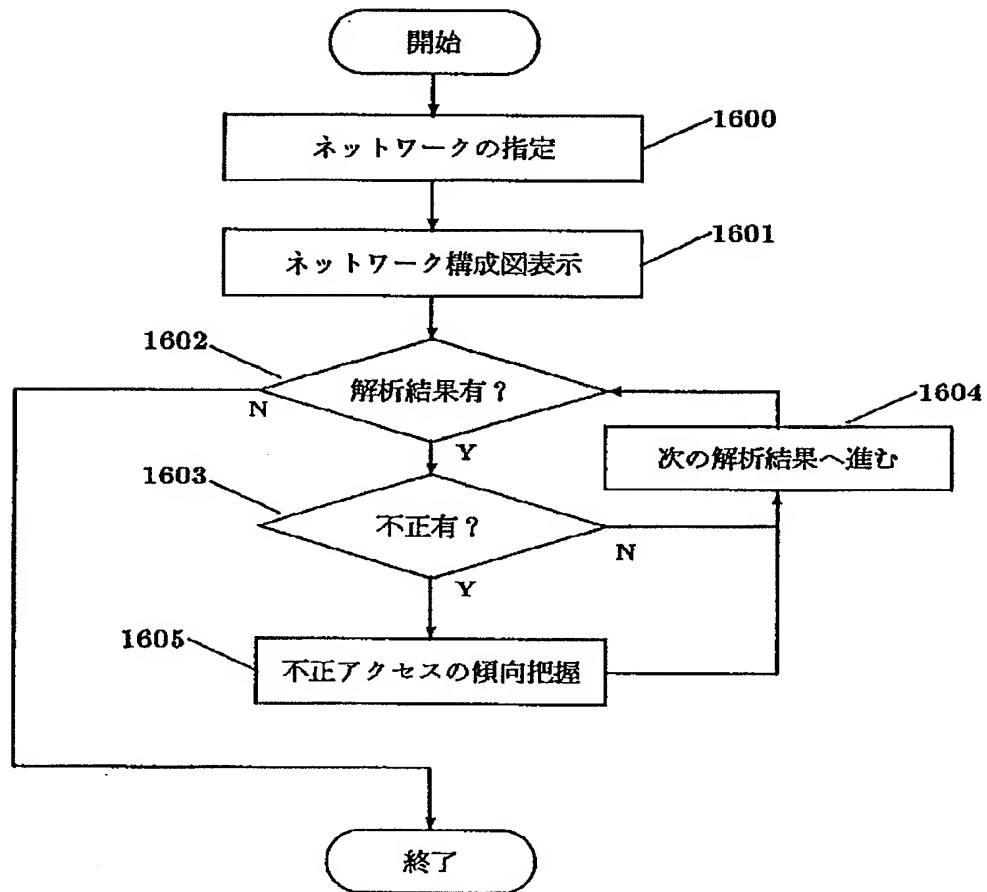
【図12】

図 1 2



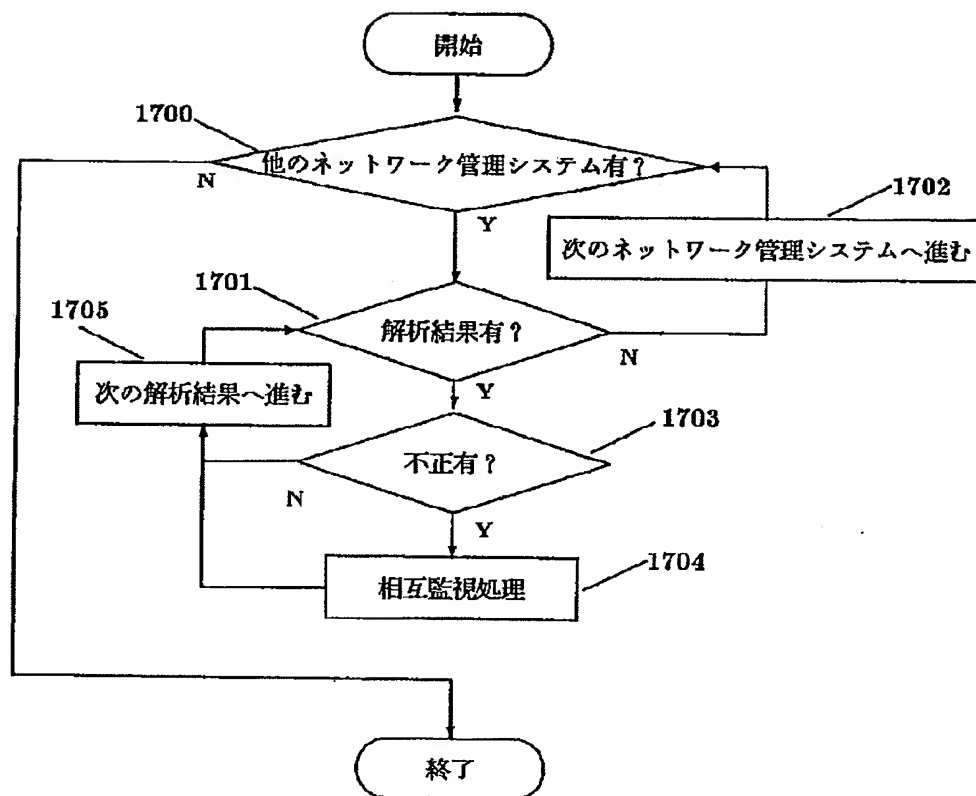
【図15】

図 15



【図16】

図 1 6



【図17】

図17

